IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

UNITED STATES OF AMERICA,	§	
	§	
	§	
VS.	§	CRIMINAL ACTION NO. 4:20-CR-455
	§	
	§	
ZHENGDONG CHENG.	§	

ORDER

Pending before the Court is Defendant Zhengdong Cheng's ("Defendant" or "Cheng") Motion to Suppress (Doc. No. 41). Defendant supplemented the Motion prior to the Government filing a response. (Doc. No. 45). The United States of America ("Government") responded to the Motion. (Doc. No. 46). Defendant then filed a reply in support of its Motion (Doc. No. 48) and USA filed a surreply in opposition to the Motion (Doc. No. 49), after which this Court held a hearing, received evidence, and heard argument. After reviewing the Motion, the arguments, the evidence, and the applicable law, the Court grants in part and denies in part the Motion.

I. Factual Background

On August 20, 2020, a criminal complaint was filed against Defendant Zhengdong Cheng charging him with wire fraud, false statements, and conspiracy. An arrest warrant was issued for Cheng on the same day. These charges were based on allegations that Cheng intentionally failed to disclose that he was employed by the Chinese University, Guandong University of Technology, in order to obtain a grant from the National Aeronautics and Space Administration (NASA). On August 23, 2020, Cheng, a professor at Texas A&M University, arrived at Easterwood Airport in College Station, Texas, returning from a work trip in Qatar. While Cheng

was retrieving his luggage from baggage claim, he was approached by Federal Bureau of Investigation ("FBI") Special Agent Michael Collier and NASA Office of Inspector General ("NASA OIG") Special Agent Todd Angle.

Agents Collier and Angle requested that Cheng follow them to a room in the airport for questioning. Shortly after detaining Cheng in the room, the agents read Cheng his *Miranda* rights. *See Miranda v. Arizona,* 384 U.S. 436 (1966). Cheng asked whether or not the agents could tell him why he was being questioned, but the agents suggested that they could not do so until Cheng waived his *Miranda* rights.[1] Cheng then stated, "But I, I, if you have—if you can get a lawyer, I want to have a lawyer present." Agent Collier responded "You are absolutely—but we just can't talk to you if you do that right now. We can't answer any of your questions right now." Cheng then asked whether he was free to go to his hotel, and Agent Collier informed him that he could not leave because he was being detained, but that he was not under arrest. At the time of his detainment, Cheng was carrying electronic devices and those were segregated by the agents.

Cheng continually sought an explanation as to why he was being detained, and the agents repeatedly reiterated that they could provide him more information only if he waived his

---

[1] The full relevant exchange was as follows:

> Agent Collier: "If you decide to answer questions now without a lawyer present, you have the right to stop at any time. Now, you're not under arrest. But we say this because you're talking to law enforcement."
>
> Cheng: "I—can you tell me you..."
>
> Agent Collier: "I, yeah! I absolutely can but I—I can't before..."
>
> Cheng: "If you have—if you can get a lawyer, I want to have a lawyer present."
>
> Agent Collier: "You are absolutely—but we just can't talk to you if you do that right now. We can't answer any of your questions right now."

(Doc. No. 46, Ex. A).

Miranda rights. Cheng asked if he would be free to leave if he requested an attorney, to which the agents responded he was not free to leave.[2] Cheng, still having derived no information about the basis for his sudden detainment, asked about the consequences of this situation, at which point the agents told him that the matter was "very serious" and that an arrest warrant has been issued for him.

Eventually, Cheng signed a written waiver of his *Miranda* rights, and the officers questioned Cheng for approximately two hours. Toward the end of the questioning, the officers asked Cheng if he would be willing to provide the passwords to some of his electronic devices. Cheng eventually consented and entered his passwords into his devices and provided the passwords to the agents. Agent Collier took the devices to a separate room, where the passwords were verified by additional agents. After the passwords were verified, the devices were placed in "airplane mode" until the agents secured search warrants to search the device. The parties agree that the actual devices were not searched until after the warrants were obtained. After the agents took the devices, Cheng was placed under arrest.

---

[2] The full relevant exchange was as follows:

> Agent Collier: "Well I—I want to hear everything you have to say. I—I need to, I want to, but I just want to make sure that you know your…"
>
> Cheng: "Yeah, so if I ask a lawyer right now…"
>
> Agent Collier: "Uh-huh"
>
> Cheng: "Can I go to hotel?"
>
> Agent Collier: "You do not—you're, you're being detained right now. Okay you can't—you're not free to go to the hotel, okay? Um—you know hopefully this won't take very long. We can try to make it quick."

(Doc. No. 46, Ex. A).

II. Discussion

Cheng argues that the statements obtained during the interrogation should be suppressed because Cheng invoked his Fifth Amendment right to counsel, and any alleged waiver of Cheng's rights made after that invocation was not knowing and voluntary. Specifically, Cheng requests that the Court suppress the entire interrogation—including his oral and written statements, his consent to search the seized electronic devices—and any evidence obtained as a result of the interrogation, including the provision of the passwords and the information obtained from the devices. The Court will address the interrogation first and the electronic devices second.

A. Admissibility of Cheng's Custodial Statements

The Fifth Amendment provides that "no person . . . shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend. V. The Supreme Court has held that, in order to safeguard the privilege against self-incrimination, the Due Process Clause requires that incriminating statements obtained during a custodial interrogation be inadmissible as evidence against a defendant unless the defendant was provided a full and effective warning of his rights. *See Miranda*, 384 U.S. at 444–45. The Government concedes that Cheng was in custody at the time of the interrogation; therefore, there is no dispute that the interrogation was custodial.

One of the rights included under *Miranda's* umbrella is the accused's right to counsel. *Miranda*, 384 U.S. at 470. "Invocation of the *Miranda* right to counsel 'requires, at a minimum, some statement that can reasonably be construed to be an expression of a desire for the assistance of an attorney.'" *Davis v. U.S.*, 512 U.S. 452, 459 (1994) (quoting *McNeil v. Wisconsin*, 501 U.S. 171, 178 (1991)). An individual may waive his or her *Miranda* rights "provided the waiver is made voluntarily, knowingly and intelligently." *Miranda*, 384 U.S. at 444. If the accused

"waives his right to counsel after receiving the *Miranda* warnings, law enforcement officers are free to question him. But if a suspect requests counsel at any time during the interview, he is not subject to further questioning until a lawyer has been made available or the suspect himself reinitiates conversation." *Davis*, 512 U.S. at 458 (internal citations omitted); *see also Edwards v. Arizona*, 451 U.S. 477, 485 (1981) (explaining that once the accused invokes his right to counsel, "the interrogation must cease until an attorney is present") (cleaned up). "Whether a suspect invoked his right to counsel is . . . a mixed question of law and fact." *Soffar v. Cockrell*, 300 F.3d 588, 592 (5th Cir. 2002).

"When a suspect makes an ambiguous or equivocal statement," officers may seek to ask clarifying questions to ensure that the suspect has actually invoked his or her right to an attorney. *Davis*, 512 U.S. at 461. "Clarifying questions help protect the rights of the suspect by ensuring that he gets an attorney if he wants one, and will minimize the chance of a confession being suppressed due to subsequent judicial second-guessing as to the meaning of the suspect's statement regarding counsel." *Id.* One cannot, however, use "clarification" as a guise for convincing a suspect to waive his or her rights. *Edwards*, 451 U.S. at 485 (explaining that "*Miranda* itself indicated that the assertion of the right to counsel was a significant event and that once exercised by the accused, 'the interrogation must cease until an attorney is present.'" (quoting *Miranda*, 384 U.S. at 474)).

The Court agrees with Cheng and finds that the agents violated Cheng's due process rights by failing terminate the interrogation after Cheng's request for counsel. Cheng's statement of "[I]f you can get a lawyer, I want to have a lawyer present" was not sufficiently ambiguous as to require clarifying questions. When a defendant clearly invokes his right to counsel, as Cheng did, officers must cease the interrogation immediately, though, as stated above, they may ask

clarifying questions to ensure that the right to counsel has actually been invoked. *Davis*, 512 U.S. at 461–62. In *Davis*, the Supreme Court held that clarifying questions were appropriate when the interrogee said, "Maybe I should talk to a lawyer." *Id.* at 455. The Court reasoned that a reasonable officer may not understand such a statement to be a request for counsel. *Id.* at 459.[3]

After Cheng's unambiguous request for a lawyer, Agent Collier immediately sought to clarify that Cheng did in fact wish to have a lawyer present. Cheng again requested a lawyer by stating "I need to have a lawyer have me [sic]," to which Collier responded, "Okay, if . . . then—then you understand then—then we're done, okay?" (Doc. No. 46). Collier's response demonstrates an understanding of Cheng's invocation of his right to counsel. Nevertheless, rather than ending the conversation until a lawyer was present, Agent Collier continued to question Cheng about whether he did in fact wish to have a lawyer present. While officers can seek clarification, they cannot then try to persuade a suspect to waive his right to counsel after the right to counsel has been invoked. *Edwards*, 451 U.S. at 485. The dialogue immediately following Cheng's request for a lawyer was clearly designed to persuade him to retract the request.[4]

Cheng's statement is a far cry from "Maybe I should talk to a lawyer." *Davis*, 512 U.S. at 455. Though Cheng does qualify his statement with "if you can get a lawyer," the remaining portion of the statement—and the entire statement taken as a whole—leaves little doubt that

---

[3] The officers in the *Davis* case ceased questioning after petitioner stated, "I think I want a lawyer before I say anything else." *Davis*, 512 U.S. at 455.

[4] When Cheng sought clarification as to the purpose and consequences of his detainment, the agents asked Cheng "You have a lot of questions, right?" When Cheng replied affirmatively, the agents stated that they could not talk to him unless he waived his right to an attorney. (Doc. No. 46, Ex. A).

"While it is assuredly good police practice to inform a person of the reason for his arrest at the time he is taken into custody, we have never held that to be constitutionally required." *Devenpeck v. Alford*, 543 U.S. 146, 155 (2004). Though not a constitutional requirement, it is important to point out that a person who has been detained has an interest, and potentially a right, to know why. Otherwise, why should a person cooperate with some unknown individuals purporting to be law enforcement?

Cheng wanted to, and did, invoke his right to have an attorney present. While this Court is not unaware of the cultural, communication barrier that the agents faced when conversing with Cheng (as is evident from the videotape), in failing to stop the interrogation after Cheng's request for an attorney, the agents violated Cheng's Fifth Amendment rights. As a result, Cheng's statements obtained as a result of the interrogation must be suppressed.

B. Admissibility of Evidence Obtained on Cheng's Devices

Cheng also contends that if his statements from the interrogation are suppressed, the results of the searches of the seized devices must also be suppressed because Cheng provided the passwords during the interrogation, and absent the passwords, the Government would have been unable to search the devices. The Government, obviously, does not agree.

Surprisingly, there is very little factually analogous case law upon which the Court may draw in its analysis. Nevertheless, in order to evaluate this argument, the Court must look to the law interpreting both the Fourth and Fifth Amendments. First, the Court must analyze whether Cheng's provision of the passwords constitutes "fruit of the poisonous tree" under the Fourth Amendment.[5] Second, the Court must analyze whether the Government could have compelled Cheng to provide access to the contents of the devices without violating his Fifth Amendment rights. The Court addresses each topic in turn.

1. Fourth Amendment

The Fourth Amendment protects "[the] right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. Searches and seizures are deemed reasonable, and therefore lawful, when they are based on probable cause and executed pursuant to a warrant. *See id*; *see also Coolidge v. New Hampshire*, 403 U.S. 443, 449 (1971). To safeguard the rights enshrined in the Fourth Amendment, the

[5] Defendant does not attack the actual possession of the devices by the agents.

Supreme Court "created the exclusionary rule, a deterrent sanction that bars the prosecution from introducing evidence obtained by way of a Fourth Amendment violation." *Davis v. United States*, 564 U.S. 229, 231–32 (2011). "Generally, the exclusionary rule prohibits the introduction at trial of all evidence that is derivative of an illegal search, or evidence known as 'fruit of the poisonous tree.'" *United States v. Hernandez*, 670 F.3d 616, 620 (5th Cir. 2012) (internal quotations and citations omitted). Both physical evidence and verbal statements are subject to the exclusionary rule. *Id.*

In the instant case, the relevant Fourth Amendment inquiry concerns the search of the seized devices following the interrogation, made possible by Cheng's provision of the passwords.[6] Importantly, none of the seized devices were searched until search warrants were obtained. The validity of these warrants has not been questioned. Cheng argues, however, that "[r]egardless of when the 'search' of the devices occurred, if [his] statements are suppressed, the passwords, like the written consent, are fruit of the poisonous tree. Absent those passwords, the Government would not have been able to image/copy the devices at that time or search the devices at any time." (Doc. No. 48).

The Court has already determined that Cheng's statements obtained as a result of the interrogation, which included the passwords for the seized devices, must be suppressed. This is not, however, the end of the analysis. The Court finds it necessary to address the question of whether Cheng's provision of the passwords renders the subsequent search of the devices inadmissible under the Fourth Amendment.

[6] It is worth noting that at least some of the seized devices belonged to Texas A&M University. The University was cooperating with the Government's investigation and presumably had the ability to access those devices and the contents contained therein. Moreover, there may be some level of uncertainty as to whether Cheng had any expectation of privacy with respect to the A&M devices. *See e.g., O'Connor v. Ortega*, 480 U.S. 709, 726 (1987); *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 760 (2010). Given this Court's ruling, it need not resolve this issue.

As earlier mentioned, the exclusionary rule made applicable to the Fourth Amendment prohibits the introduction of ill-gotten evidence at trial. *Hernandez*, 650 F.3d at 620. The exclusionary rule, however, is not without exceptions. One such exception is the inevitable discovery doctrine. *United States v. Zavala*, 541 F.3d 562, 579 (5th Cir. 2008). The Court understands that neither side has briefed whether the "inevitable discovery doctrine" applies in this case. Nevertheless, a discussion of the doctrine is necessary in order to bridge the gap between Defendant's "fruit of the poisonous tree" argument, on the one hand, and the Government's Fifth Amendment arguments on the other.

The inevitable discovery doctrine "renders the exclusionary rule inapplicable to otherwise suppressible evidence if that evidence would inevitably have been discovered by lawful means." *United States v. Jackson*, 596 F.3d 236, 241 (5th Cir. 2010). The inevitable discovery doctrine applies if "(1) there is a reasonable probability that the contested evidence would have been discovered by lawful means in the absence of police misconduct and (2) the Government was actively pursuing a substantial alternate line of investigation at the time of the constitutional violation." *Id.*[7]

The key question here, of course, is whether the contents of the devices would have been "inevitably discovered" without Cheng's voluntary provision of the passwords. Due to the fact that the devices were password-protected, there are presumably two ways (besides Cheng's provision of the passwords during the interrogation) in which the devices could be unlocked or decrypted. On the one hand, the Government could have utilized various means to gain entry to the device without knowing the password. It has done this in other cases. *See e.g., United States*

[7] It appears clear that the Government was actively pursuing many substantial alternate lines of investigation, as evidenced by its Complaint (Doc. No. 1) leading to the arrest warrant, its subsequent search warrant applications, and the fact that it had already obtained the ongoing cooperation with Texas A&M University. Moreover, there has been no argument that the Government was not pursuing alternate lines of investigation.

v. Fulton, 192 F.Supp.3d 728, 730 (S.D. Tex. 2016) ("Because the phone was password protected, it took approximately one year for the government to gain entry into the device."). Although theoretically possible, there is no evidence in the record to suggest that there is a reasonable probability that the government would have been able to do so in the instant case.

On the other hand, the Government could have sought a court order to compel Cheng to either provide the passwords, or alternatively, compel Cheng to decrypt the devices as part of the search warrant. This approach raises a Fifth Amendment concern: whether compelling Cheng to provide the decrypted devices would qualify as a "testimonial" act and thereby result in a violation of his Fifth Amendment privilege against self-incrimination. Therefore, before the Court can determine whether the contents of the devices would have been "inevitably discovered," it must address this Fifth Amendment concern.

2. Fifth Amendment

The Fifth Amendment provides that "No person . . . shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend. V. This applies "only when the accused is compelled to make a Testimonial Communication that is incriminating." *Fisher v. United States*, 425 U.S. 391, 408 (1976). The question here, then, is whether compelling Cheng to provide the passwords or to provide the devices in an unencrypted state would qualify as a "testimonial communication that is incriminating." *Id.*[8] To answer this Fifth Amendment

[8] The Court is aware that there is a factual distinction between the agents obtaining the passwords during an interrogation and a situation where the Government obtains a court order compelling the defendant to provide the passwords or an unencrypted device; however, in the instant case they are functionally equivalent, because if the Court could compel the decryption, the evidence would inevitably be discovered just as if the defendant had provided the passwords in an interrogation. Consequently, the Court will address the likely results of a hypothetical Government motion to compel in order to determine the applicability the inevitable discovery doctrine.

question, we find guidance by looking to the "act of production" and "foregone conclusion" doctrines.[9]

a. Act of Production Doctrine

In *Fisher*, the Supreme Court held that the Fifth Amendment privilege against self-incrimination is not violated when the government compels a person to turn over incriminating evidence, unless the act of production is both "testimonial" and "incriminating." 425 U.S. at 409–10; *see also United States v. Spencer*, No. 17-cr-00259, 2018 WL 1964588, at *1 (N.D. Cal. Apr. 26, 2018). There is no Fifth Amendment issue, however, where the act of production "adds little or nothing to the sum total of the Government's information" because that means that the existence and the location of the documents sought to be produced are a "foregone conclusion." *Fisher*, 425 U.S. at 411.

A rule prohibiting the government from ever compelling decryption of a password-protected device would certainly lead to absurd, untenable results. "Whether a defendant would be required to produce a decrypted drive would hinge on whether he protected that drive using a fingerprint key or a password composed of symbols. . . . [or] whether he kept the documents at issue in a combination safe or a key safe." *Spencer*, 2018 WL 1964588, at *2; *see also New York v. Quarles*, 467 U.S. 649, 671 (1984) (O'Connor, J., concurring in part); *United States v. McAuley*, 563 F. Supp. 2d 672, 678 (W.D. Tex. 2008), *aff'd*, 420 F. App'x 400 (5th Cir. 2011) (explaining that a password on a computer "is simply a digital lock"). The application of the Fifth Amendment should not be dependent on the manner in which an individual locks or secures material, whether physically or electronically.

The first question, then, is whether there was, or would be, an "act of production" here. In the *Spencer* case, the Government sought an order to compel the defendant to decrypt the seized

[9] Given the nature of the inevitable discovery doctrine, the Court must conduct this analysis in the hypothetical.

devices. 2018 WL 1964588, at *1. That being the case, the court was not required to analyze the seizure under the Fourth Amendment. In this case, the Government has not sought an order to compel the Cheng to decrypt the seized devices because it obtained the passwords during the August 20th interrogation. Despite this factual distinction, the *Spencer* analysis and reasoning is useful as it relates to the Fifth Amendment concerns at issue. The *Spencer* decision found that the government's request for decrypted devices required an act of production. *Id.* at *2. This Court, like the *Spencer* court, concludes that a governmental request for decrypted devices and the respondent's compliance with the subsequent court order constitutes an act of production. In this case, Cheng essentially "produced" unencrypted devices by providing both the devices and the passwords to the agents. Given these controlling facts, in can hardly be argued that Cheng did not engage in an act of production.

The next question is whether the act of production would violate Cheng's Fifth Amendment privilege against self-incrimination. As mentioned, this privilege applies "only when the accused is compelled to make a Testimonial Communication that is incriminating." *Fisher v. United States*, 425 U.S. 391, 408 (1976). Acts of production "may certainly communicate information about the existence, custody, and authenticity" of the documents or information being compelled. *United States v. Hubbell*, 530 U.S. 27, 36 (2000). There is little doubt that compelling Cheng to unlock the devices would be communicative. There is also little doubt that compelling Cheng to unlock the devices could eventually lead to incriminating evidence, as the devices may allow the Government to discover an immeasurable amount of pertinent material in the form of emails, text messages, photographs, call records, and other communications. The Court finds, however, that the act of production is not testimonial.

A communicative act "must itself, explicitly or implicitly, relate a factual assertion or disclose information" in order to be testimonial. *Doe v. United States*, 487 U.S. 201, 210 (1988). This Court finds that Cheng's compelled provision of the passwords, or production of the unlocked devices, would not disclose any information or relates any factual assertion, other than the undisputed fact that Cheng controlled the devices. Here, Cheng clearly possessed the devices, gave his devices to the Government, and told the Government that he has access to the devices. As a result, compelling Cheng to provide the passwords or to unencrypt the devices is not testimonial and, as a result, does not infringe on Cheng's Fifth Amendment rights. There are other courts that have found that an act of production may "represent incriminating testimony within the meaning of the Fifth Amendment" in certain circumstances when that act could amount to a representation that a defendant has the ability to decrypt the devices, making it more likely that the defendant encrypted the devices himself, suggesting that the defendant was the individual who put the contents of the devices on the devices themselves. *Spencer*, 2018 WL 1964588, at *2. Such a result is more likely testimonial (and thus protected by the Fifth Amendment) in a crime where, unlike in this case, the mere possession of the computer's contents constitutes the crime.

The Government argues that Cheng's provision of the passwords is not testimonial and does not implicate the Fifth Amendment because his knowledge of the passwords is a "foregone conclusion." Therefore, to determine whether compelling Cheng to either provide the passwords or to provide the devices in an unencrypted state could be considered "testimonial," so as to invoke the Fifth Amendment privilege against self-incrimination, the Court analyzes the "foregone conclusion" doctrine.

b. Foregone Conclusion Doctrine

A compelled act of production does not present a Fifth Amendment self-incrimination issue where the act of production "adds little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411. The "foregone conclusion" doctrine provides:

> The Fifth Amendment does not protect an act of production when any potentially testimonial component of the act of production—such as the existence, custody, and authenticity of evidence—is a "foregone conclusion" that "adds little or nothing to the sum total of the Government's information." [*Fisher*, 425 U.S. at 411]. For the rule to apply, the Government must be able to "describe with reasonable particularity" the documents or evidence it seeks to compel." [*Hubbell*, 530 U.S. at 30].

United States v. Apple MacPro Computer, 851 F.3d 238, 247 (3d. Cir 2017); *see also* Orin S. Kerr and Bruce Schneier, *Encryption Workarounds* (March 22, 2017), 106 GEO. L.J. 989 (2018) ("The foregone conclusion doctrine teaches that, if the testimonial aspect of an act of production is already known to the government and is not proven to be proven by the testimonial act, the testimony is a foregone conclusion and the Fifth Amendment privilege does not apply."). The relevant question here, then, is whether it is a "foregone conclusion" that Cheng knew the passwords to the seized devices.

As mentioned, there is relatively little factually analogous case law addressing this situation. Some guidance is provided in *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012). In that case, a defendant invoked his Fifth Amendment privilege against self-incrimination when asked to comply with a subpoena to produce unencrypted contents of certain hard drives that were believed to contain child pornography. *Id.* at 1337–38. The district court issued an order granting the defendant immunity for the act of production of the unencrypted devices—but not for derivative use of the contents—and requiring

him to respond to the subpoena. *Id.* The Eleventh Circuit held that by complying with the order, the defendant would "certainly use the contents of his mind to incriminate himself or lead the Government to evidence that would incriminate him." *Id.* at 1349.[10] Further, the circuit court held that the "foregone conclusion" doctrine would not apply because, unlike in the current case, the Government failed to show any basis for its belief that the defendant either had access to the relevant encrypted information, or that he was even capable of decrypting the files. *Id.*[11] While not precisely the same factual scenario, the analysis is pertinent here.

In *In re Grand Jury Subpoena*, the Eleventh Circuit held that when seeking to compel a defendant to provide a decrypted or unlocked device, the government must show that it is a "foregone conclusion" that (1) the defendant has the ability to decrypt the device[s]; and (2) there are certain files on the device(s). 670 F.3d at 1346.[12] Importantly, the Eleventh Circuit relied on precedent derived from *Fisher,* which analyzed the government requesting specific documents pursuant to a subpoena rather than a warrant. This is a key distinction, because "[c]ompliance with the subpoena tacitly concedes the existence of the [documents] demanded and their possession or control" by the defendant. *Fisher*, 425 U.S. at 410. As the *Spencer* court noted, turning over "decrypted devices would not be tantamount to an admission that specific files, or any files for that matter, are stored on the devices, because the government has not asked for any specific files." *Spencer*, 2018 WL 1964588, at *3. Setting aside the later obtained search

[10] One must keep in mind that the alleged illegal act in *In re Grand Jury Subpoena* was possession of child pornography—a crime proven by its mere possession. 670 F.3d 1335.

[11] The Eleventh Circuit went on to hold that the district court could have compelled the defendant to turn over the unencrypted contents had they not "erred in limiting [the defendant's] immunity . . . to the Government's use of his act of decryption and production." *Id.* at 1349–50.

[12] The Eleventh Circuit did not discuss the question of allowing the Government to compel the defendant to decrypt the relevant device because the Government failed to demonstrate any prior knowledge that the files in question existed, or where they were. *Id.* at 1347. In this case, however, the Complaint makes clear that the Government was aware that certain contents, such as emails, in all probability would be found on Cheng's electronic devices. (*See* Doc. No. 1).

warrants which contained specific topics that the government was pursuing, the Government—as in the *Spencer* case—did not asked for specific files or contents on the devices. Rather, the Government has asked for the devices themselves, and access to them. One must keep in mind that mere possession of the devices/contents in this case is not a factor in the alleged crimes, unlike the charges at issue in *In re Grand Jury Subpoena*. As a result, the Government must only demonstrate that it is a foregone conclusion that Cheng has the ability to decrypt the devices. This can be demonstrated through independent knowledge, thus negating any question concerning Fifth Amendment privilege.[13]

In order to complete the "foregone conclusion" analysis, courts have grappled with the standard of proof required to demonstrate that a defendant has the ability to decrypt the devices. In other contexts, courts have applied a "reasonable particularity" standard, requiring the government to establish independent knowledge "of the existence, possession, and authenticity of subpoenaed documents with 'reasonable particularity' before the communication inherent in the act of production can be considered a foregone conclusion." *United States v. Hubbell*, 167 F.3d 552, 579 (D.C. Cir. 1999), *aff'd*, 530 U.S. 27 (2000); *see e.g., In re Grand Jury Subpoena*, 670 F.3d at 1349; *Apple MacPro Computer*, 851 F.3d at 247. Another court has used a "preponderance of the evidence" standard when evaluating the government's knowledge as it related to a "foregone conclusion." *United States v. Fricosu*, 841 F.Supp.2d 1232, 1234 (D. Colo. 2012).

In *Spencer*, the court determined that the appropriate standard to be applied in determining whether knowledge of passwords is a foregone conclusion is "clear and convincing

[13] *See* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767, 783 (2019) (explaining "when investigators present a suspect with a password prompt, and they obtain an order compelling the suspect to enter in the correct password, the suspect cannot have a valid Fifth Amendment privilege if the government independently can show that the suspect knows the password").

evidence." *Spencer*, 2018 WL 1964588, at *3. The court reasoned that the reasonable particularity standard is ill-suited with respect to compelling decryption because "a defendant's ability to decrypt is not subject to the same sliding scale [as physical evidence evaluated under the reasonable particularity standard]. He is either able to do so, or he is not." *Id.*[14]

This Court need not determine the requisite standard in this case. Here, there is little dispute that the seized devices belonged to Cheng or were in his possession. There is no dispute that the seized devices were being used by Cheng. Put simply, the uncontroverted evidence establishes that devices were controlled by Cheng at the time he was detained. It is, by any standard, a foregone conclusion that Cheng knew the passwords for each of the seized devices at the time of his arrest. Since his knowledge of the passwords was a foregone conclusion, and since the mere possession of the devices and/or their contents was not a crime, an order compelling Cheng to provide the devices in an unencrypted state would be neither "testimonial" nor "incriminating," and would not violate Cheng's Fifth Amendment right against self-incrimination.[15] Therefore, the Government would have been able to compel Cheng to decrypt the seized devices once the search warrants were issued. Since they would have been able to compel Cheng to produce the passwords or the devices unencrypted, the inevitable discovery doctrine applies, and the results of the search of the devices are not "fruit of the poisonous tree."

To summarize, it was a foregone conclusion that Cheng knew the passwords to the seized devices; thus, his acts of producing the devices and the passwords would not qualify as "incriminating testimony" in violation of his Fifth Amendment privilege against self-

[14] The *Spencer* court also astutely noted that "'reasonable particularity' is not really an evidentiary standard at all. It is better viewed as a substantive standard that helps to ensure that any testimony at issue really is a 'foregone conclusion.'" 2018 WL 1964588, at *3. This Court agrees.

[15] This analysis would, of course, be different if the alleged crime involved the mere possession of materials or documents found on the seized device. If, for example, a defendant was charged with possession of child pornography such as in *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, the act of turning over the decrypted devices would likely be "tantamount to an admission" and thus testimonial.

incrimination. Moreover, the possession of the devices and/or the passwords that facilitated access was not testimonial. Consequently, the Government would have been able to have a court compel him to decrypt the devices. It follows, then, that the Government would have been able obtain a court order to compel Cheng to provide the passwords, and the contents of the devices would have been "inevitably discovered." Since the evidence obtained from the seized devices would have been inevitably discovered, the inevitable discovery doctrine exception to the Fourth Amendment's exclusionary rule applies to the devices, and the contents retrieved from them need not be suppressed as "fruit of the poisonous tree.

III. Conclusion

For the foregoing reasons, the Court hereby grants in part and denies in part Defendant's Motion to Suppress (Doc. No. 41). The Court finds that Defendant sufficiently invoked his right to counsel during the August 23, 2020, interrogation, and any statements obtained as a result must be suppressed. The Court, however, denies the motion with respect to information obtained from the seized electronic devices.

Signed at Houston, Texas, this 12th day of January, 2022.

Andrew S. Hanen
United States District Judge